



Mark Burnett

IT security analyst and author working in application security, passwords, authentication, and identity. Based in South Weber, Utah <https://xato.net>

Mar 16, 2017 · 5 min read

The \$5 Million Password



Last summer at BSides Las Vegas I spent most of my time watching talks on the Passwords track, which probably isn't much of a surprise to many of you—passwords are kind of my thing. There are a number of us who faithfully attend these talks and we are a familiar sight to each other. But unless you were paying close attention may not have noticed a slightly older woman with long silvering hair quietly sitting near the back. Although she appeared a bit out of place, she was taking meticulous notes.

Later that day, after I gave my own presentation, this woman approached me and asked if she could have a few minutes to ask me some questions. I agreed and she began asking me questions about cracking passwords, the current state of technology available, and what technological advances I expected in the near future.

Seeing my confusion with her line of questioning, she explained her situation. A year earlier she learned about the Ethereum platform and decided to invest some money purchasing Ether—about \$18,000 (USD) worth. At the time it was an amount that she felt comfortable

risking but since then her life situation changed and she wanted to cash it out.

Working from her hand-written list of current passwords, she came up with a 12-character random sequence of letters, numbers, and punctuation.

The problem she faced now was because of how she set her wallet password when purchasing the Ether. A beginner, she got confused during the process and thought that the password was a one-time crypto value she needed to enter and then destroy. Working from her hand-written list of current passwords, she came up with a 12-character random sequence of letters, numbers, and punctuation. She set the password, then immediately destroyed the paper she wrote it down on.

So now a year had passed and she needed the money but when she went to cash out was shocked seeing the current value of her wallet: about \$1.2 million (USD). Of course, shortly after her heart sank as she realized that she needed that original password she had destroyed. Not only was she not getting the gains she had earned, but would also lose her original investment. Desperate for any solution, she ran across the BSides Las Vegas passwords track and flew out to attend.

Now in the last week we saw a big rally in altcoin prices. Ethereum, at the time of writing, is jumped to \$28 yesterday and now has risen to \$44 today. This puts the value of her wallet at over \$5 million. And the price is going up by the minute (future person reading this see the current price here).

By the time she spoke to me, she had already received enough information from others to realize there was little hope of recovering her password. Still, she wasn't ready to give up until she had explored all her options.

This is what we knew about her password:

- It was exactly 12 characters long
- It contained mostly lowercase letters, a few numbers, and symbol or two

- All characters would exist on a US English keyboard (a total of 95).
- It was random, but not computer-generated—she chose it herself
- She had a list of other passwords she chose that might reveal a pattern

Given these parameters we know that there are a maximum of 95^{12} or 540,360,087,662,636,962,890,625 possible passwords; only one of which was hers. Even with the capability of trying a billion passwords per second—well beyond the current capabilities—it would take you over 17,000,000 years to crack the password.

Now seeing her desperation, I wondered if there was any way to reduce this number. There were, after all, some unique traits we knew about her password.

For example, she was pretty confident she only used punctuation from the numbers row on the keyboard and definitely wouldn't have used parenthesis. I began adding up all the possible combinations we could eliminate when I was given a bit of a sanity check by @Sc00bzT, who was participating in the conversation: it doesn't matter how much I eliminate, the password is still uncrackable. I was reminded just how hard it is for us humans to comprehend huge numbers.

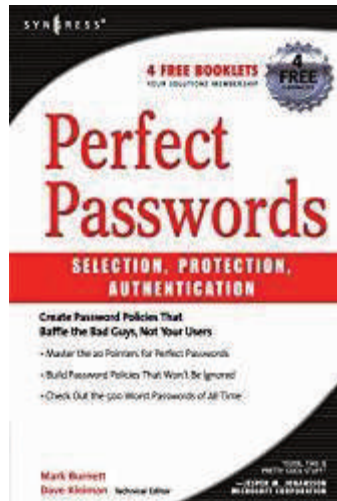
For sake of illustration, let's go through the math. First, we know we can eliminate certain characters. With lowercase and uppercase letters, numbers, and eight possible symbols, we are down to 70^{12} or 13,841,287,201,000,000,000,000 possible passwords.

We know that there are exactly 12 characters, which means we can eliminate all passwords from 1 through 11 characters. That would allow us to subtract 70^{11} or more passwords.

If you start thinking about it, there are actually billions or even trillions more passwords you could eliminate. For example, she told me she would never have used two symbols next to each other which would allow us to eliminate all those possibilities. Following this strategy, we could possibly eliminate 90% of the possible passwords.

But is that enough? Even removing this massive chunk of possibilities, we are still left with about 1,384,128,720,100,000,000,000 passwords to try. In fact, even if you could eliminate 99.9999% of the possibilities, you are still left with about 1,384,128,720,100,000,000 passwords you need to try. Even with a billion computers hammering away trying a billion passwords per second, this would take a very, very, very long time and generate quite a bit of CPU heat.

In the meantime this wallet is nothing but a black hole of bits, growing in value until some point in the future where this password might be crackable. Advances in CPU power will never get us there, the only hope is a flaw in the crypto itself.



Mark Burnett is a security consultant and author of the book Perfect Passwords

